

## UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

FILED  
Asheville

Dec 08 2020

U.S. District Court  
Western District of N.C.

In the Matter of the Search of

Apple ID "Kyle Burns," and email and iCloud  
storage account for [waterBuffalo224@icloud.com](mailto:waterBuffalo224@icloud.com)  
stored at the premises owned, maintained,  
controlled, and operated by Apple, Inc., 1 Infinite  
Loop, Cupertino CA 95014

Case No.1:20-mj-00071

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A to the accompanying Affidavit.

located in the \_\_\_\_\_ Northern \_\_\_\_\_ District of \_\_\_\_\_ California \_\_\_\_\_, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B to the accompanying Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. 2252A  
18 U.S.C. 2251

Offense Description  
Possession, Receipt, Distribution of Child Pornography  
Production of Child Pornography

The application is based on these facts:

See accompanying Affidavit.

- ☒ Continued on the attached sheet.  
☐ Delayed notice \_\_\_\_\_ days (give exact ending date if more than 30 \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Scheafer M. Farmer

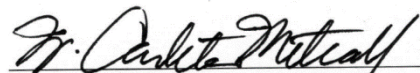
Applicant's signature

Scheafer M. Farmer, HSI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P 4.1 by (telephone)

Signed: December 8, 2020



W. Carleton Metcalf  
United States Magistrate Judge



Date: 12/8/2020



## **AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, Scheafer M. Farmer, being duly sworn, state as follows:

### **INTRODUCTION**

1. I am a Special Agent (SA) with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been so employed from August 1998, to the present. I am currently assigned to the HSI Hendersonville, North Carolina office. As part of my official duties, I have conducted and participated in investigations related to the sexual exploitation of children. I have also received training and instruction in the field of investigating child pornography to include distribution and possession. As part of my duties and responsibilities as an HSI SA, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18 United States Code, Section 2251, et seq.

2. This affidavit is submitted in support of an application for a search warrant for information contained in, or associated with, Apple ID “Kyle Burns” and the email and iCloud storage accounts of “waterBuffalo224@icloud.com,” controlled by the web-based electronic communication service provider known as Apple Inc. This affidavit is submitted under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), and Rule 41, Federal Rules of Criminal Procedure, requiring Apple Inc., to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account(s) referenced in this affidavit and further described in Attachment A, including the contents of communications. Apple Inc. is located at 1 Infinite Loop, Cupertino, California 95014. The facts in this affidavit are based on my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of the facts known by me about this investigation.

3. I have probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, involving the use of a computer and the Internet, is located in and within the aforementioned account. I have probable cause to believe that the member account that is the subject of this application will have stored information and communications that are relevant to this investigation, including evidence of the identity of the person maintaining the account and other email accounts associated with the email account and iCloud account of “waterBuffalo224@icloud.com” Based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in the account(s).

#### **STATUTORY AUTHORITY**

4. This investigation concerns alleged violations of Title 18, United States Code, Sections 2251 and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, federal prosecutors, and computer forensic examiners, I know the following:

a. 18 U.S.C. § 2251(a) in pertinent part makes it a federal crime or offense for any person to employ, use, persuade, induce, entice or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction if that person knew and had reason to know that such visual depictions would be transmitted using a means and facility of interstate commerce, that is, by computer via the internet.

b. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing or accessing with intent to view any visual depiction of minors engaging in sexually explicit

conduct using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails.

c. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

d. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to knowingly possess or knowingly access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer.

e. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

5. The legal authority for this search warrant application is derived from Rule 41, Federal Rules of Criminal Procedure and Title 18, United States Code, Sections 2701 et seq., titled "Stored Wire and Electronic Communications and Transactional Records Access."

6. Title 18, United States Code, Section 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703(a) & (b), as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

### **DEFINITIONS**

7. The following definitions apply to this Affidavit:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the

production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to,

keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that



creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" may refer to an IP address of "149.101.1.32." Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

l. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. A "Preservation Letter" is a letter that a government entity may issue to internet service providers pursuant to Title 18, United States Code, Section 2703(f), to ensure that the internet service providers preserve records in their possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

n. "Cloud storage" is an online central storage location, which allows users to access their files from anywhere using a device connected to the Internet.

- o. “iCloud” is a cloud storage and cloud computing service from Apple Inc.

The service allows users to store data on remote computer servers for download to multiple devices, to include smart phones and computers.

### **COMPUTERS AND CHILD PORNOGRAPHY**

8. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

9. The development of computers has radically changed the way that child pornographers obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

10. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, the images can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos

indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

12. The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, Apple Inc., and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also

be retained unintentionally, *e.g.*, traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as “chat logs.” Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as “chatting,” or “instant messaging.”

15. Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic “chat logs” often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. In addition to electronic communication, a computer user’s internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

#### **INFORMATION REGARDING APPLE INC. EMAIL AND ICLOUD ACCOUNTS**

16. Through my training and experience, as well as review of materials provided to me by Apple Inc. and other experienced law enforcement officers, I have learned that Apple Inc. provides a variety of online services, including electronic mail (“email”) access, to the general public. Apple Inc. allows subscribers to obtain email accounts at the domain name “iCloud.com” like the email account listed in Attachment A. Subscribers obtain an account by registering

online with Apple Inc. During the registration process, Apple Inc. requires subscribers to provide basic personal information. Therefore, the corporate servers of Apple Inc. are likely to contain stored electronic communications (including retrieved and un-retrieved email for iCloud subscribers) and information concerning subscribers and their use of Apple Inc. and iCloud services, such as account access information, email transaction information, and account application information.

17. I have learned that an email that is sent to an Apple Inc. iCloud subscriber, is stored in the subscriber's "Inbox" on Apple Inc. servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Apple Inc. servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Apple Inc. and other cloud storage services, such as Google Drive, Dropbox, and SkyDrive, have provided their users with larger storage capabilities associated with the user's account. Apple Inc. starts users out with 5 gigabytes of storage space, and if the user begins to fill that space up, the user can pay for additional storage space. Based on my training and experience, and conversations with other law enforcement officers with experience in executing search warrants of email accounts, I know that search warrants for email accounts and computer media may reveal stored emails sent and/or received long prior to the date of the search.

18. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that when the subscriber sends an email, it is initiated at the user's computer, transferred via the internet to Apple Inc.'s servers, and then transmitted to its end destination. Apple Inc. often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Apple Inc. servers, the email can remain on the system indefinitely.

19. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that a sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Apple Inc., but may not include all of these categories of data.

20. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that an iCloud subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, videos and other files on servers maintained and/or owned by Apple Inc. Subscribers to an iCloud account might not store on their home computers copies of the emails stored in the iCloud account. This is particularly true when they access their iCloud account through the web, or if they do not wish to maintain particular emails or files in their residence. In essence, a subscriber's email box has become a common online data storage location for many users.

21. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that in general, email providers like Apple Inc. require that each of their subscribers provide certain personal identifying information when registering for an email account. This information could include the subscriber's full name, physical address, telephone numbers and other identifiers, such as alternative email addresses, and, for paying subscribers, means and source of payment (including a credit card or bank account number).

22. Based on my training and experience, I know that email providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records

of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account associated with Apple Inc.'s website(s)), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account, as well as the geographic location of these devices.

23. Based on my training and experience, I know that in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications.

24. Based on my training and experience, I know individuals often use email accounts for everyday transactions because it is fast, low-cost, and simple to use. People use email to communicate with friends and family, manage accounts, pay bills, and conduct other online business. Email users often keep records of these transactions in their email accounts, to include identifying information such as name and address.

25. Based on my training and experience, I know that evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and other files.

26. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that an Apple ID is an all-in-

one email address that is used to log into various online systems that Apple Inc. offers for many of its products. Users of Apple Inc. products such as "iTunes" and "Photostream" can have one Apple ID that corresponds to their accounts, and one of the services available through Apple Inc. is iCloud storage. Apple Inc. offers the ability to link all of its products through an iCloud account.

27. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that iCloud is a file hosting, storage, and sharing service that is provided for iCloud account users. iCloud has been integrated into Apple Inc. and is linked to, associated with, and accessible using an iCloud email account. The integration allows users to directly upload documents and photos within the iCloud account, store them on iCloud, and share with other users.

28. Based on my training and experience, as well as information provided to me by Apple Inc. and other experienced law enforcement officers, I know that an Apple Inc. iCloud account allows users to upload files, photos, and favorites on Apple Inc. servers to cloud storage, and allows members to access them from any computer with an Internet connection. After uploading photos and/or files to iCloud, one can share the photos and other files with friends or to anyone on the iCloud network. The user can send an email, using the user's iCloud email account, to other individuals inviting them to view the photos and files. The service allows the user to keep the files private, share only with specific contacts, or make the files public. Publicly shared files do not require an Apple Inc. iCloud account to access; the service offers five (5) gigabytes of free personal storage.

#### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

29. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain



common characteristics are often present in individuals who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals, who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents in the area of investigating cases involving sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other likeminded individuals over the Internet. As such, they tend to maintain or “hoard” their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. Based on my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often maintain and/or possess the items listed in Attachment B.

30. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials.

31. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collection of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

**BACKGROUND OF INVESTIGATION AND  
FACTS ESTABLISHING PROBABLE CAUSE**

32. On June 9, 2020, Detective Pam Cannon with the Polk County Sheriff's Office (PCSO) received a report related to a possible Child Exploitation/Obscene material case. An individual named Tyler Grant Schlabach had reported that while he was working on a computer for his friend Steve SEYMOUR, he discovered a file containing a picture of a "shirtless child." Schlabach reported that he opened the file and discovered that it contained a large number of pictures of naked males approximately 6 to 14 years of age. Schlabach reported that he was not sure how to proceed, so he contacted his father for advice. Schlabach reported his father instructed him to contact Staff Attorney JJ Suave at the Polk County Sheriff's Office.

33. Deputy Lance Johnson (PCSO) went to Schlabach's residence and retrieved the computer hard drive and placed it into evidence.

34. On June 9, 2020, Detective Cannon contacted Schlabach in order to clarify some of the information. Schlabach stated that he had known SEYMOUR since childhood and provided a telephone number and address for SEYMOUR. Schlabach informed Detective Cannon that at the time he discovered the file containing the concerning images he had been working on SEYMOUR's computer and that SEYMOUR had removed the original "hard drive" from the system. Schlabach stated he was reinstalling a drive brought to him by SEYMOUR for more storage space on the computer.

35. On June 10, 2020, Detective Cannon executed a search warrant for SEYMOUR's Toshiba Solid State M.255D hard drive, which Schlabach had been working on. Special Agent (SA) and Computer Forensic Analyst William Meadows conducted a forensic examination of the hard drive and was able to open multiple files for inspection. SA Meadows discovered approximately 200 files located on the hard drive containing graphic material of juvenile males

engaged in sexually explicit activity. SA Meadows also discovered an account username for the computer of “Kyle Burns.”

36. Detective Cannon contacted Schlabach in the presence of SA Meadows. Detective Cannon asked Schlabach if he was aware of the name “Kyle Burns.” Schlabach stated that SEYMOUR wanted him to set up a fictitious name on the computer and suggested “Kyle Burns.” Schlabach provided Detective Cannon with the same spelling for the username that was discovered during SA Meadow’s examination. Schlabach stated that he had also set up the original computer back in September 2019, and he was not sure that the “bio clock” was on the correct time. Schlabach further stated that he assembled the computer and set up the fake username at the request of SEYMOUR.

37. Based on the volume and nature of the hard drive’s content, Detective Cannon applied for and was granted a search warrant for SEYMOUR’s residence at 101 E. Lake Shore Drive, Tryon, North Carolina 28782.

38. On June 11, 2020, Detective Cannon executed the search warrant at SEYMOUR’s residence. During the course of the search, Detective Cannon and members of the Polk County Sheriff’s Office discovered numerous electronic storage devices and a hand written note with the following information on it:

Apple Id Name Kyle Burns  
waterBuffalo224@icloud  
pass jB@ra2xzEfx223  
“B and E are capital”.

39. The name “Kyle Burns” discovered on the handwritten note at SEYMOUR’s residence is the same computer username discovered during the forensic analysis of SEYMOUR’s hard drive by SA Meadows and corroborated by Tyler Schlabach.

40. On November 3, 2020, your affiant served Apple, Inc. with a preservation letter for the records related to Apple ID “Kyle Burns” and iCloud email [waterBuffalo224@icloud.com](mailto:waterBuffalo224@icloud.com).

41. SEYMOUR has been in custody on related state charges since June 2020.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

42. I anticipate executing this warrant pursuant to the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Apple Inc. to disclose to the government copies of the records and other information (including the content of communications) more particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, authorized persons will review that information to locate the items described in Section II of Attachment B.

**REQUEST FOR ORDER TO KEEP ACCOUNT ACTIVE**

43. Because the investigation is ongoing, I would further request the Court to order Apple Inc. to continue to maintain the Apple ID “Kyle Burns” and email account and iCloud storage of [waterBuffalo224@icloud.com](mailto:waterBuffalo224@icloud.com), in an open and active status.

**CONCLUSION**

44. Based on my training and experience, and the facts as set forth above, I have probable cause to believe that on the computer systems in control of Apple Inc., there exists evidence of a crime(s), contraband and/or fruits of a crime(s). Specifically, I have probable cause to believe that the Apple ID “Kyle Burns” and the email account and iCloud storage account of [waterBuffalo224@icloud.com](mailto:waterBuffalo224@icloud.com), described in Attachment A, will contain evidence,

fruits, and instrumentalities of a crime(s), that is violations of Title 18, United States Code, Sections 2251, 2252, and 2252A. Accordingly, a search warrant is requested.

45. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711(3), and Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." Title 18, United States Code, Section 2711(3)(A)(i).

46. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

/S/ Scheafer M. Farmer  
Date: December 7, 2020  
Special Agent  
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 8<sup>th</sup> day of December, 2020, at 2:03 pm.

Signed: December 8, 2020



W. Carleton Metcalf  
United States Magistrate Judge



## **ATTACHMENT A**

### **DESCRIPTION OF LOCATION TO BE SEARCHED**

This warrant applies to information contained in and associated with the Apple Inc., Apple ID “Kyle Burns” and email account and iCloud storage account of "waterBuffalo224@icloud.com," which is stored at the premises owned, maintained, controlled, and operated by Apple Inc., 1 Infinite Loop, Cupertino, California 95014.



## **ATTACHMENT B**

### **DESCRIPTION OF ITEMS TO BE SEIZED**

#### **I. Information to be disclosed by Apple Inc.**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple Inc., Apple Inc. is required to disclose the following information to the government for the account(s) listed in Attachment A. Such information should include the following:

1. The contents of all emails, instant messages and/or other communications stored in the email account for “waterBuffalo224@icloud.com” and associated with Apple ID “Kyle Burns” for the period from January 1, 2020 through the current date, including copies of emails and instant messages sent to and from the account, draft emails and instant messages, the source and destination addresses associated with each email and/or instant message, the date and time at which each email/instant message was sent, and the size and length of each email/instant message;
2. Any and all deleted emails, instant messages and/or other communications that are still maintained and/or preserved by Apple Inc., including any information described in paragraph 1 above for the period from January 1, 2020 through the current date;
3. Any and all photographs, videos, visual depictions, instant messages or other content stored in the iCloud account for “waterBuffalo224@icloud.com” and associated with Apple ID “Kyle Burns,” and all information pertaining to the source of such photographs, videos, visual depictions, messages, and other stored content for the period from January 1, 2020 to the current date, including any and all photographs, videos, visual depictions, instant messages

or other content that the user may have deleted or attempted to delete but that are still maintained and/or preserved by Apple Inc.;

4. All records or other information regarding the identification of the account for the period from January 1, 2020 to the current date, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

5. All records or other information stored by any individual using the account, including profile, address books, contact and buddy lists, calendar data, pictures, and files for the period from January 1, 2020 to the current date;

6. All records pertaining to communications between Apple Inc., and any person regarding the account, including contacts with support services and records of actions taken for the period from January 1, 2020 to the current date.

7. All records associated with other services provided with an iCloud account, to include iCloud, Groups, Office, Photos, Spaces, iTunes and iPhone for the period from January 1, 2020 to the current date.

## **II. Information to be seized by the government**

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code,

Sections 2251, 2252, and 2252A, and also including, for the account(s) listed on Attachment A, the following items:

1. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the account(s) listed on Attachment A;
2. Evidence of who used, owned, or controlled the account(s) listed on Attachment A;
3. Evidence of the times that the account(s) listed on Attachment A was used;
4. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.

### **III. By Order of the Court**

1. Pursuant to Title 18, United States Code, Section 2705(b), the Court orders Apple Inc., not to notify any person of the existence of this warrant for 180 days from service of this attachment.
2. The Court further orders Apple Inc., to continue to maintain Apple ID “Kyle Burns” and the email account and iCloud storage account of waterBuffalo224@icloud.com in an open and active status, so as not to disrupt this ongoing investigation.